## CLAIMS

What is claimed is:

1. A method for tracking a secure boot in a computer system, wherein the computer system comprises a plurality of devices, the method comprising the steps of:

(a) providing an embedded security system (ESS) in the computer system, wherein the ESS includes at least one boot platform configuration register (PCR) and a shadow PCR for each at least one boot PCR;

(b) initiating a platform reset to boot the computer system via BIOS;

(c) generating a measurement value for a device of the plurality of devices booted in the computer system;

(d) extending the measurement value to one of the at least one boot PCRs and to the corresponding shadow PCR; and

(e) comparing the measurement value of each of the at least one boot PCRs with the measurement value of the corresponding shadow PCR, wherein the computer system is trusted if the measurement values match.

2. The method of claim 1, wherein the step of providing an ESS (a) further comprises providing a Trusted Platform Module (TPM) in accordance with a Trusted Computing Platform Alliance (TCPA) compliant computer system.

3. The method of claim 1, wherein the initiating step (b) further comprises the step of :

(b1) resetting the measurement value in each of the at least one boot PCRs to zero;

(b2) hashing code in the BIOS to produce a BIOS digest value;

(b3) extending the BIOS digest value to one of the at least one boot PCRs and to the corresponding shadow PCR; and

(b4) executing the code in the BIOS.

4. The method of claim 3, wherein the generating step (c) further comprises the steps of:

(c1) hashing code in the device to produce the measurement value for the device.

5. The method of claim 4, wherein the extending step (d) further comprises the step of:

(d1) executing the code in the device after extending the measurement value; and

(d2) booting a trusted operating system.

6. The method of claim 5 further comprising the step of:

(f) performing preventative operations to restore trust in the computer system if the measurement values are different.

7. The method of claim 6, wherein the performing step (f) further comprises the

steps of:

(f1) executing a virus protection program.

8. The method of claim 6 further comprising the step of:

(g) resetting each of the corresponding shadow PCRs to zero once trust is established in the computer system.

9. The method of claim 8, wherein the resetting step (g) further includes the step of:

(g1) providing a secure means for resetting the shadow PCRs, whereby only an authorized entity is capable of resetting the shadow PCRs.

10. The method of claim 1, wherein the initiating step (b) further includes the step of:

(b1) performing one of a cold boot, hardware boot, and warm boot.

11. A computer readable medium containing programming instructions for tracking a secure boot in a computer system, wherein the computer system comprises a plurality of devices, the programming instructions for:

(a) providing an embedded security system (ESS) in the computer system, wherein the ESS includes at least one boot platform configuration register (PCR) and a shadow PCR for each at least one boot PCR;

(b) initiating a platform reset to boot the computer system via BIOS;

(c) generating a measurement value for a device of the plurality of devices booted in the computer system;

(d) extending the measurement value to one of the at least one boot PCRs and to the corresponding shadow PCR; and

(e) comparing the measurement value of each of the at least one boot PCRs with the measurement value of the corresponding shadow PCR, wherein the computer system is trusted if the measurement values match.

12. The computer readable medium of claim 11, wherein the instruction of providing an ESS (a) further comprises providing a Trusted Platform Module (TPM) in accordance with a Trusted Computing Platform Alliance (TCPA) compliant computer system.

13. The computer readable medium of claim 11, wherein the initiating instruction (b) further comprises the instructions for:

(b1) resetting the measurement value in each of the at least one boot PCRs to zero;

(b2) hashing code in the BIOS to produce a BIOS digest value;

(b3) extending the BIOS digest value to one of the at least one boot PCRs and to the corresponding shadow PCR; and

(b4) executing the code in the BIOS.

14. The computer readable medium of claim 13, wherein the generating instruction (c) further comprises the instructions for:

(c1) hashing code in the device to produce the measurement value for the device.

15. The computer readable medium of claim 14, wherein the extending instruction (d) further comprises the instructions for:

(d1) executing the code in the device after extending the measurement value; and

(d2) booting a trusted operating system.

16. The computer readable medium of claim 15 further comprising the instruction for:

(f) performing preventative operations to restore trust in the computer system if the measurement values are different.

17. The computer readable medium of claim 16, wherein the performing instruction (f) further comprises the instruction for:

(f1) executing a virus protection program.

18. The computer readable medium of claim 16 further comprising the instruction for:

(g) resetting each of the corresponding shadow PCRs to zero once trust is established in the computer system.

19. The computer readable medium of claim 18, wherein the resetting instruction (g) further includes the instruction for:

(g1) providing a secure means for resetting the shadow PCRs, whereby only

an authorized entity is capable of resetting the shadow PCRs.

20. The computer readable medium of claim 11, wherein the initiating instruction (b) further includes the instruction for:

(b1) performing one of a cold boot, a hardware boot, and a warm boot.

21. A system for tracking a secure boot in a computer system, wherein the computer system comprises a plurality of devices, the system comprising:

a processor in the computer system;

an embedded security system (ESS) coupled to the processor via a secure bus, wherein the ESS includes at least one boot platform configuration register (PCR) and a shadow PCR for each at least one boot PCR;

a BIOS coupled to the processor for booting a device of the plurality of devices in the computer system;

wherein the BIOS generates a measurement value for the device of the plurality of devices and extends the measurement value to one of the at least one boot PCRs and to the corresponding shadow PCR, and wherein the measurement values of the at least one boot PCRs is compared to the measurement values of the corresponding shadow PCRs to determine whether the computer system is trusted.

22. The system of claim 21, wherein the ESS comprises a Trusted Platform Module (TPM) in accordance with a Trusted Computing Platform Alliance (TCPA) compliant computer system.

23. The system of claim 21, wherein the measurement value in the at least one boot PCRs are reset to zero at initiation of a boot sequence, and wherein prior to executing code in the BIOS, BIOS code is hashed to produce a BIOS digest value, which is extended to one of the at least one boot PCRs and the corresponding shadow PCR.

24. The system of claim 23, wherein the BIOS generates the measurement value for the device by hashing code in the device.

25. The system of claim 24, wherein after the measurement value has been extended, a trusted operating system is booted by executing the code in the device .

26. The system of claim 25, wherein the trusted operating system compares the measurement values of the at least one boot PCRs and the corresponding shadow PCRs, and performs preventative operations to restore trust in the computer system if the measurement values differ.

27. The system of claim 26, wherein the trusted operating system launches a virus protection program if the measurement values differ.

28. The system of claim 26, wherein the trusted operating system resets each of the corresponding shadow PCRs to zero once trust is established in the computer system.

29. The system of claim 28 further comprising:

means for allowing only the trusted operating system to reset the shadow PCRs.